

DETAILED ACTION

1. An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.
2. Authorization for this Examiner's Amendment was given in a telephone interview with Applicant's representative, Mr. Steven Smith (Reg. No. 36,684) on February 23, 2011. During the telephone conference, Mr. Smith has agreed and authorized the Examiner to amend Claims 4, 16-17, 22, 39-40, and 51-52.

Claims

3. Replacing Claims 4, 16-17, 22, 39-40, and 51-52 as following:

Claim 4: (Currently Amended) The method of claim 51, further comprising transferring MIPv6-related information from the **home** AAA server in the home network to a home agent.

Claim 16: (Currently Amended) The method of claim 4, wherein the MIPv6-related information is transferred from the **home** AAA server in the home network to the home agent in an AAA framework protocol application.

Claim 17: (Currently Amended) The method of claim 16, wherein the home agent is a local home agent in the visited network and the MIPv6-related information is transferred from the home AAA ~~home~~ server to the local home agent via [[an]] the visited AAA server in the visited network.

Claim 22: (Currently Amended) The method of claim 19, further comprising building, at the mobile device, a home address for the mobile device using at least a portion of the address of its assigned home agent; and transferring the home address of the mobile device from the mobile device to the home AAA ~~home network~~ server in the home network using a round trip of a selected EAP procedure.

Claim 39: (Currently Amended) The system of claim 52, wherein MIPv6-related information is transferred from the home AAA server in the home network to a home agent in an AAA framework protocol application.

Claim 40: (Currently Amended) The system of claim 39, wherein the home agent is a local home agent in the visited network and the MIPv6-related information is transferred from the home AAA ~~home~~ server to the local home agent via [[an]] the visited AAA server in the visited network.

Claim 51: (Currently amended) A method of authentication and authorization support for Mobile IP version 6 (MIPv6), comprising the steps of:

encrypting Extensible Authentication Protocol (EAP) authentication and authorization information in a mobile device operating in a visited network;

sending the encrypted EAP authentication and authorization information from the mobile device to a pass-through **visited** Authentication, Authorization, and Accounting (AAA) client in the visited network utilizing a protocol for carrying authentication information for network access;

forwarding the encrypted EAP authentication and authorization information from the pass-through **visited** AAA client to a pass-through visited AAA server in the visited network;

forwarding the encrypted EAP authentication and authorization information from the pass-through visited AAA server in the visited network to a home AAA server in the mobile device's home network;

performing an analysis of the encrypted EAP authentication and authorization information by the home AAA server;

sending a MIPv6-related challenge message from the home AAA server to the mobile device via the pass-through visited AAA server and the pass-through **visited** AAA client in the visited network based on the analysis of the encrypted EAP authentication and authorization information;

sending a MIPv6-related challenge response message from the mobile device to the home AAA server via the pass-through visited AAA client and the pass-through visited AAA server in the visited network;

performing an analysis of the challenge response message contents by the home AAA server; and

sending a MIPv6-related authentication and authorization results message from the home AAA server to the mobile device reporting a result of the analysis of the challenge response message contents and providing session parameter information;

wherein the pass-through visited AAA client and the pass-through visited AAA server forward all messages in a pass-through manner in which information within Type and Type-Data ~~header~~ fields ~~are~~ after EAP layer headers is not examined by the pass-through visited AAA client and the pass-through visited AAA server;

whereby prior EAP encryption is applied between the mobile device and the home AAA server.

Claim 52: (Currently Amended) A system for authentication and authorization support for Mobile IP version 6 (MIPv6), comprising a mobile device operating in a visited network, a pass-through Authentication, Authorization, and Accounting (AAA) visited client in the visited network, a pass-through visited AAA server in the visited network, and a home AAA server in the mobile device's home network, wherein the system performs the steps of:

the mobile device encrypting Extensible Authentication Protocol (EAP) authentication and authorization information;

the mobile device sending the encrypted EAP authentication and authorization information to the pass-through visited AAA client in the visited network utilizing a protocol for carrying authentication information for network access;

the pass-through visited AAA client forwarding the encrypted EAP authentication and authorization information to the pass-through visited AAA server in the visited network;

the pass-through visited AAA server forwarding the encrypted EAP authentication and authorization information to the home AAA server in the mobile device's home network;

the home AAA server performing an analysis of the encrypted EAP authentication and authorization information;

the home AAA server sending a MIPv6-related challenge message to the mobile device via the pass-through visited AAA server and the pass-through visited AAA client in the visited network based on the analysis of the encrypted EAP authentication and authorization information;

the mobile device sending a MIPv6-related challenge response message to the home AAA server via the pass-through visited AAA client and the pass-through visited AAA server in the visited network;

the home AAA server performing an analysis of the challenge response message contents; and

the home AAA server sending a MIPv6-related authentication and authorization results message to the mobile device reporting a result of the analysis of the challenge response message contents and providing session parameter information;

wherein the pass-through visited AAA client and the pass-through visited AAA server forward all messages in a pass-through manner in which information within Type and Type-Data header fields are after EAP layer headers is not examined by the pass-through visited AAA client and the pass-through visited AAA server;

whereby prior EAP encryption is applied between the mobile device and the home AAA server.

Examiner's Statement of reason of Allowance

4. **Claims 4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52 are allowed.**
5. **The following is an examiner's statement of reasons for allowance:**

The present invention is directed to a method and system for authentication and authorization support for Mobile IP version 6, wherein Extensible Authentication Protocol (EAP) is utilized between a mobile device and the home Authentication, Authorization, and Accounting (AAA) server, wherein pass-through visited AAA client and pass-through visited AAA server forward all messages in a pass-through manner in which information within Type and Type-Data fields after EAP layer headers is not

examined by the pass-through visited AAA client and the pass-through visited AAA server, so that prior EAP encryption is applied between the mobile device and the home AAA server.

The closest prior art, as previously recited, Faccin et al., ("Faccin," US 2002/0120844), Palekar et al., ("Palekar," US 2002/0120844), and Akhtar et al., ("Akhtar," US 7,079,499) are also generally directed to various aspects of authentication and authorization for mobile network. However, none of Faccin, Palekar, and Akhtar teaches or suggests, alone or in combination, the particular combination of steps or elements as recited in the independent claims, claims 51 and 52. For example, none of the cited prior art teaches or suggest the steps of "sending the encrypted EAP authentication and authorization information from the mobile device to a pass-through visited Authentication, Authorization, and Accounting (AAA) client in the visited network utilizing a protocol for carrying authentication information for network access; forwarding the encrypted EAP authentication and authorization information from the pass-through visited AAA client to a pass-through visited AAA server in the visited network; forwarding the encrypted EAP authentication and authorization information from the pass-through visited AAA server in the visited network to a home AAA server in the mobile device's home network; sending a MIPv6-related challenge message from the home AAA server to the mobile device via the pass-through visited AAA server and the pass-through visited AAA client in the visited network based on the analysis of the encrypted EAP authentication and authorization information; sending a MIPv6-related challenge response message from the mobile device to the home AAA server via the pass-

through visited AAA client and the pass-through visited AAA server in the visited network; sending a MIPv6-related authentication and authorization results message from the home AAA server to the mobile device reporting a result of the analysis of the challenge response message contents and providing session parameter information; wherein the pass-through visited AAA client and the pass-through visited AAA server forward all messages in a pass-through manner in which information within Type and Type-Data header fields are after EAP layer headers is not examined by the pass-through visited AAA client and the pass-through visited AAA server; whereby prior EAP encryption is applied between the mobile device and the home AAA server. ”

Therefore the claims are allowable over the cited prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437